DEVELOPMENT OF SECURE AND VERIFIABLE COLOR VISUAL CRYPTOGRAPHY SCHEMES

A

Research Synopsis

Submitted to

School of Computational Science

Swami Ramanand Teerth Marathwada University,

Vishnupuri, Nanded

in partial fulfillment for the Registration of the degree, Doctor of Philosophy in Computer Science (Faculty of Computer Science & Technology)

Submitted By

Mr. D. R. Somwanshi
School of Technology, SRTM University Nanded, Sub Center-Latur

Under the guidance of

Dr. Vikas T. Humbe
Assistant Professor,
School of Technology,
Swami Ramanand Teerth Marathwada University,
Sub-Centre, Ausa Road, Peth Latur,(MS) 413512.

February- 2018

Table of Contents

Abstract: 1
1. Introduction 2
2. Review of Literature & Development in the Subject 4
I. Review Based on types of Visual Cryptography: 4
II. Review Based on Visual Cryptography Schemes 5
3. Goals and Objectives of Research/ Proposed Hypothesis: 8
4. Methodology to be adopted: 9
5. Importance of study/ Society application 11
6. Proposed Work Design/Formulation and structure of study: 12
7. References 13

DEVELOPMENT OF SECURE AND VERIFIABLE COLOR VISUAL CRYPTOGRAPHY SCHEMES

Abstract:

Visual Cryptography is a special cryptographic technique in which the decryption can perform by the human visual system. In this technique the information or secret image to be encrypted is divided into *n* different parts or share. Each part or share is then distributed among the *n* different users, and then we can specify at least *k* out of *n* shares is required to get the original information. Visual cryptography is specially designed for data security or providing more secure method for allowing access to more sensitive data. It simply used for user authentication for providing access to data. Recently many Secrets Sharing Scheme of visual cryptography schemes are developed ranging from *(2, 2)* Visual Cryptography Scheme to Segment based Visual Cryptography Scheme. So many different types of visual cryptography are also developed ranging from Halftone Visual Cryptography to Progressive Multi-resolution Visual Cryptography. But there are so many problems of visual cryptography such as pixel expansion, alignment problem, extensive codebook design, Cheating Prevention, Flipping Issues, Distortion Problem, Thin Line Problems and lossy recovery are quiet unresolved.

This study is aims to explore the various visual cryptography schemes, to analyze the performance of different visual cryptographic scheme, to presents the in-depth description of how visual cryptographic scheme (VCS) such as pixel expansion, contrast mapping and cheating prevention works. Finally to provide the promising solutions to secure and verifiable secrete sharing scheme for color images to overcome the problems such as complexity in computation, prevention from cheating, storage requirement, quick transmission over networks and superimposing the verified secrete color image without distortion and thin line problem.

1. Introduction

Visual Cryptography (VC) is a technique of encrypting the written material such as printed text, handwritten notes, images etc. in a perfectly secure way and which can be decoded directly by human visual system [1]. It means decryption is not required or huge amount of calculation is not required to decrypt the text. This allows everybody to make use of the system, even if they don't have sufficient knowledge about encryption or decryption of cryptography and fail to carry out any computations.

This technique is first introduced by Naor et al. [1], in 1994. In this technique the message or image data to be protected or encrypted is divided into *n* different parts or share. Each part or share is distributed among the *n* different users, and then we can specify at least *k* out of *n* shares are stacked together or required to get the original information. The *k-1* shares cannot be used to generate the original message. For example suppose there are six thieves wanted to share a bank account, but they don't trust on one another because of that, they divided up the password for the account in such a way that, any three or more thieves working together can have access to account, but not less than three thieves can access the account.

In Visual Cryptography each pixel of the images is divided into smaller blocks. There are always the same numbers of white and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks [1, 3, and 4]. The example figure 1.1 uses pixels that are divided into two parts.

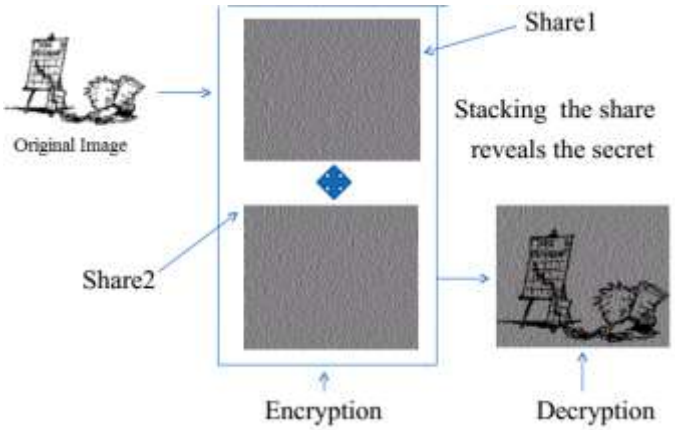


Figure 1.1: Visual Cryptography Scheme

Sharing important documents over network using this technique is now more essential, because of universal use of internet in almost every filed. In this era of electronic commerce, it is more important to provide information security to every individual. For protecting the security of

information different encryption technique of traditional cryptography are being used. Using such technique, information to be transmitted from one location to another is encrypted into cipher text and latter it is decrypted or recovered by using correct key but the key and decryption algorithms can be guessed by unauthorized user or professional intruder. To provide the solution for this visual cryptography schemes are now being used widely.

Visual Cryptography is categorized into five major types: In Halftone Visual Cryptography image is made up of a series of dots rather than a continuous tone. These dots can be different sizes, different colors, and sometimes even different shapes. Larger dots are used to represent darker more dense areas of the image, while smaller dots are used for lighter areas [4].

The half toning method degrades the quality of the original image. In Visual Cryptography with perfect restoration both gray and color images are encoded without degradation. It retains the advantages of traditional visual cryptography. Here the stacking operation involves only XORing [3, 4].

In Color Visual Cryptography Color decomposition of color channels in color image are performed and then the gray scale half toning for each channel is performed or the color half toning first followed by the Color decomposition is performed [2].

To enhance the resolution of constructed image Multi-resolution Visual Cryptography is used. In traditional *(k;n)* visual cryptography, if the threshold k number of shares are available then the image of single resolution is constructed. In progressive visual cryptography scheme, by stacking the threshold number of shares together, reconstructed image is formed and resolution of the final image is enhanced using other shares [4, 8].

With these types of visual cryptography so many Secrets Sharing Scheme are also used such as (2, 2) Visual Cryptography Scheme, (k, n) Visual Cryptography Scheme, Recursive Threshold Visual Cryptography Scheme, Segment based Visual Cryptography Scheme etc.

Each type of scheme and each type of visual cryptography has its own advantages of disadvantages. There are some problems of visual cryptography such as Complexity in computation, alignment problem, cheating with shares, storage requirement, quick transmission over networks and superimposing the verified secrete image without distortion and thin line problem are still need to be resolved. To provide the solution for these problems, this study is planned to provide the more powerful solutions to security of information using novel methods in secure and verifiable colored visual cryptography.

2. Review of Literature & Development in the Subject

Review of Literature and development in the subject is related to this study categorized into two main parts: types of Visual Cryptography and Secret Sharing Scheme.

I. Review Based on types of Visual Cryptography:

Zhi Zhou et.al [5] proposed a novel technique named halftone visual cryptography to achieve visual cryptography via halftoning. Their method is based on the blue-noise dithering principles, and it utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation proposed by them shows that the visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method.

Zhongmin Wang et.al [6] works on Halftone Visual Cryptography via error diffusion in their method the secret image is concurrently embedded into binary valued shares while these shares are halftoned by error diffusion-the workhorse standard of halftoning algorithms. Error diffusion has low complexity and provides halftone shares with good image quality. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images.

Young-Chang Hou [2] works on Color visual cryptography and proposes three methods for visual cryptography of gray-level and color images based on past studies in black and white visual cryptography, the halftone technology, and the color decomposition method. Their method retain the advantages of black-and-white visual cryptography, which exploits the human visual system to decrypt secret images without computation, and also have the backward compatibility with the previous results in black-and-white visual cryptography, such as the t out of n threshold scheme.

Vandana Purushothaman and Sreela Sreedhar [7] work on pixel expansion and poor image quality. They introduce the effective technique of share generation based on XOR-based visual cryptography for General Access Structures and succeed in Perfect restoration of the secret, no pixel expansion and no code book requirement is needed and they finally use generated shares to cover in an image using steganography which provides additional security.

Jin et al. [8] proposed a multi-resolution approach to share secret image that can be applied to VC. They expand pixels to 3×3 blocks in which eight of them are used to represent the gray

value of each pixel and the remaining one is used to store the halftone value of the secret image. In order to take advantage of visual effects, Jin et al. uses a "lookup table" to adjust the pixel value so that pixels with a larger gray value in the secret image of more *"1"*s (*1* represents black) in its eight bit-planes. The adjusted eight binary digits are handled by conventional VC; therefore, an obscure secret image can be directly obtained from stacking shares. By utilizing computer equipment's to perform the XOR operations on the ninth bit, the halftone secret image can be perfectly reconstructed. However, Jin's work cannot disclose the secret image progressively. At most, we can say that they proposed a multi-resolution scheme via different approaches to share a secret image. Their method expanded every secret pixel to a *3×3* block, and by using the pixel-expansion scheme, their shares will be further expanded to *6×6* times larger, which causes a severe waste of storage and transmission time.

Young-Chang Hou and Zen-Yu Quan [9] work on Progressive Visual Cryptography and proposed a brand new sharing scheme of progressive VC to produce pixel unexpanded shares. In their research, the possibility for either black or white pixels of the secret image to appear as black pixels on the shares is the same, which approximates to *1/n*. Therefore, no one can obtain any hidden information from a single share, hence they ensures the security. When superimposing *k* (sheets of share), the possibility for the white pixels being stacked into black pixels remains *1/n*, while the possibility rises to *k/n* for the black pixels, which sharpens the contrast of the stacked image and the hidden information, therefore, become more and more obvious. After superimposing all of the shares, the contrast rises to *(n − 1)/n* which is apparently better than the traditional ways that can only obtain 50% of contrast, consequently, a clearer recovered image can be achieved.

II. Review Based on Visual Cryptography Schemes

In *(2, 2)* Visual Cryptography Scheme, original image is divided into *2* shares. Each pixel in original image is represented by non-overlapping block of *2* or *4* sub-pixels in each share. Anyone, having only one share will not be able to reveal any secret information. Both the shares are required to be superimposed to reveal the secret image [1].

In *(2, 2)* visual cryptography, both the shares are required to reveal secret information. If one share gets lost due to some technical problem, secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal information and user cannot afford to lose a single share. To give some flexibility to user, basic model of visual cryptography proposed by

Naor and Shamir can be generalized into a visual variant of *k* out of *n* visual cryptography scheme [1].

In *(k, n)* visual cryptography scheme, all *n* shares have equal importance. Any *k* out of *n* shares can reveal the secret information. It may compromise the security of system. To overcome this problem, G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extended *(k, n)* visual cryptography model to general access structure [10]. In general access structure scheme, given set of *n* shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any *k* shares from qualified subset of shares can reveal secret information, but less than *k* shares from qualified subset of shares can not reveal any secret information. Even *k* or more shares from forbidden set can‟t reveal secret information. So, Visual cryptography for general access structure improves the security of system.

In *(k, n)* visual secret sharing scheme, a secret of *"b"* bits is distributed among *"n"* shares of size at least *"b"* bits each. Since only *k* out of *n* shares is needed to reveal secret, every bit of any share conveys at most *1/k* bits of secret. It results in inefficiency in terms of number of bits of secret conveyed per bit of shares. To overcome this limitation Abhishek Parakh and Subhash Kak proposed "Recursive threshold visual cryptography" [11]. The basic idea behind Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to *(n-1)/n* bit of secret which is nearly100%.

Chang-Chou Lin, WenHsiang Tsai proposed visual cryptography for gray level images [12]. In this scheme a dithering technique is used to convert gray level image into approximate binary image. Then existing visual cryptography schemes for binary images are applied to create the shares

Visual cryptography schemes were applied to only black and white images till year 1997. Verheul and Van Tilborg proposed first color visual cryptography scheme [13]. In this visual cryptography scheme one pixel is distributed into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black. F.Liu, C.K.Wu, X.J. Lin proposed a new approach for colored visual cryptography scheme [14].

All the previous researches in visual cryptography were focused on securing only one image at a time. Wu and Chen [15] were first researchers, who developed a visual cryptography scheme to

share two secret images in two shares. In this scheme, two secret binary images can be hidden into two random shares, namely *A* and *B*, such that the first secret can be seen by stacking the two shares, denoted by $A \otimes B$, and the second secret can be obtained by rotating 90 degree anti-clockwise. Shyu , Tzung-Her Chen and , Chang-Sian Wu [16,17] proposed a scheme for multiple secrets sharing in visual cryptography, where more than two secret images can be secured at a time in two shares.

Nakajima, M. and Yamaguchi, Y., developed Extended visual cryptography scheme (EVCS) [18]. An extended visual cryptography (EVC) provide techniques to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography.

D. Jin, W. Q. Yan, and M. S. Kankanhalli [8] works on progressive visual cryptography scheme, they suggested that it is not necessary to have at least *k* shares out of *n*, as in *(k, n)* secret sharing scheme. If more than one share obtained, it starts recovering the secret image gradually. The quality of recovered image improves, as the number of shares received increases.

Ran-Zan Wang [19] developed a scheme "Region Incrementing Visual cryptography" for sharing visual secrets of multiple secrecy level in a single image. In this scheme, different regions are made of a single image, based on secrecy level and different encoding rules are applied to these regions.

Bernd Borchert [20] proposed a new scheme which is not pixel-based but segment-based. They suggested that it useful to encrypt messages consisting of symbols represented by a segment display. For example, the decimal digits *0, 1, ..., 9* can be represented by seven-segment display . The advantage of the segment-based encryption is that, it may be easier to adjust the secret images and the symbols are potentially easier to recognize for the human eye and it may be easier for a non-expert human user of an encryption system to understand the working.

Feng Liu et.al [21] discuss some of the problems of visual cryptography such as Alignment Problems, cheating in presenting shares, flipping issues, distortion problems and thin line problem.

Zheng D, et.al [22] introduces a visual cryptography scheme which replicates the principle of fountains. The scheme introduced by them two advantages: non-distortion and flexible (in case of pixel expansion), presented scheme can be applied to any VCS that is under the pixel by pixel encryption model [22], such as VCS for general access structure, color VCS and extended VCS.

Feng Liu et.al [23] proposed two multi-pixel encryption size invariant visual cryptography schemes (ME-SIVCS's) which improve the visual quality of the recovered secret image by reducing the variance of the darkness levels. In addition, they also the proposed ME-SIVCS's can be used to encrypt fine secret images since they avoid some known thin line problems [23].

Shivendra Shivani and Suneeta Agarwal [24] proposed a novel verifiable progressive visual cryptography with additional embedding capacity in each share which is used for self-embedding authentication data, copyright information along with confidential payload. This embedded information in a share can be retrieved and verified at the time of any conflict. They eliminate many unnecessary encryption constraints of visual cryptography like pixel expansion, noise-like shares, explicit requirement of codebook and restriction on number of participants etc.

Shivendra Shivani [25] further works on verifiable multi-tone visual cryptography and proposes a scheme for securely transmitting the confidential images on web, they also provides cheating prevention, since each pixel of shares contains a self-embedding verifiable bit for integrity test of that pixel and finally they improve the constraints like random shares, codebook requirement, contrast loss etc.

3. Goals and Objectives of Research/ Proposed Hypothesis:

This research proposal is mainly designed to provide the ultimate, accurate, and fast solution to verifiable color secrete sharing scheme for color images and various problems of visual cryptography such as cheating prevention, distortion, pixel expansion and flipping issues using the novel scheme. Also for utilizing our technological knowledge to assists people, to solve the problems regarding information security.

Objectives of this research proposal are:

1. To provide the overview of the emerging Verifiable Color Visual Cryptography (VCVC) based on the previous related work.
2. To provide the efficient and more accurate solutions to various problems and different challenges of VCVC.
3. To design and implement a new VCVC Scheme in order to secure an image transmission and cheating prevention for colored images.

4. Minimizing the problems such as pixel expansion, distortions, flipping issues, cheating prevention and thing line problems of various secrete sharing scheme.
5. To Evaluate and analyze the performance of proposed VCVC Scheme to clarify the efficiency and quality of final image in comparison to recent related work, and finally to contribute in recommendation and assumption for the future development.

4. Methodology to be adopted:

The proposed research is focused on secure and verifiable colored visual cryptography scheme for information security. In this research study we are planned to provide the solution for cheating prevention and *k* out of *n* sharing problem.

In *k* out *of n* sharing problem consider the set P of *n* participants, the visual secrete image S is encrypted or divided in to *"n"* shadow images, these are called shares or parts where each participants gets a share to be used for getting the original message or visual image. The original message will be visible only *k* or more than *k* is combined or superimposed together. Less than *k* cannot be used for getting the original message. Sometimes the fake or illegal share can also be provided by cheaters to superimpose the shares for getting original information. For cheating prevision this study is planned for provide the verifiable share to be superimposed.

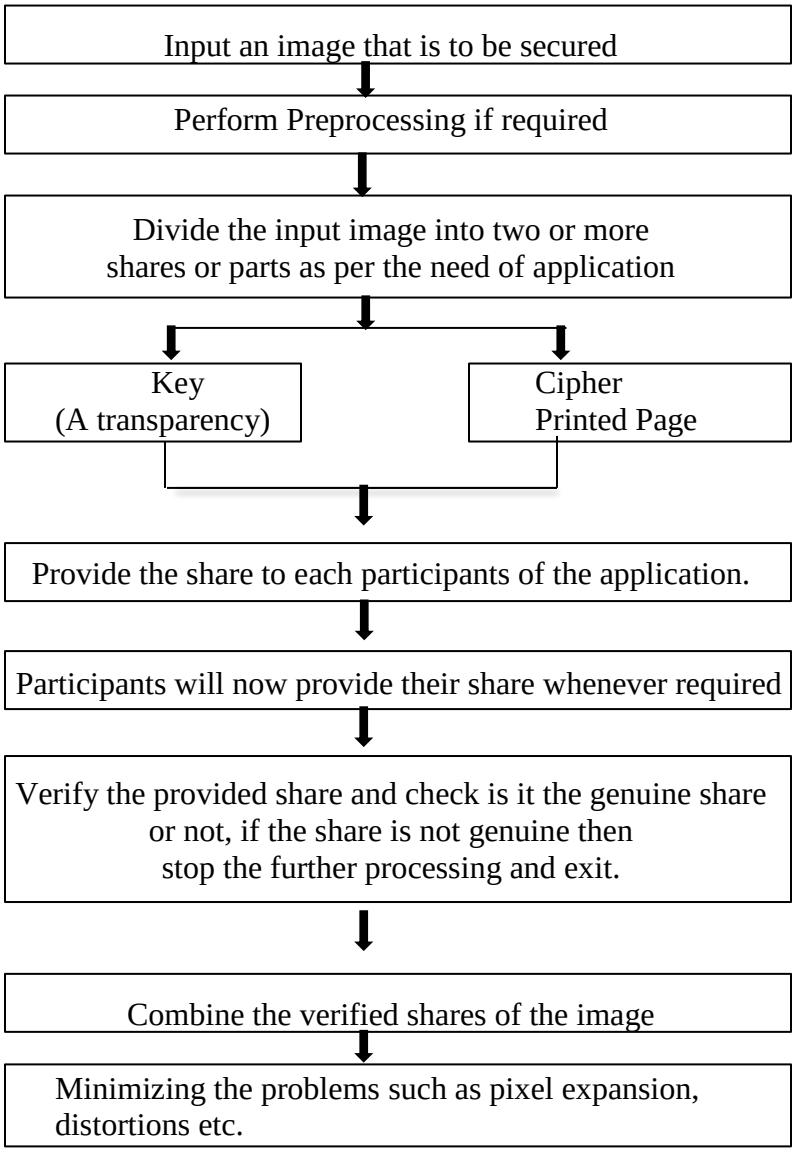
While working on color images, color channel in the color image need to be separated. For this study, RGB and CMY color model is decided to be used for color image encryption and distributing the share among participants and finally only the verifiable share will be provided for superimposing the share.

Consider the message consists of a collection of black and white pixels and each pixel is handled separately. Each share of participant is a collection of *m* black and white sub-pixels. The resulting picture can be assumed as a *[n x m]* Boolean matrix $S = [s, i, j]$

We can consider that $s, i, j = 1$ if the j^{th} sub-pixel in the i^{th} share is black and $s\ i, j = 0$ if the j^{th} sub-pixel in the i^{th} share is white.

The proposed methodology is as shown in figure 4.1. The information that is to be secure or the image that is to be protected is taken as input. Various applications such as biometric security, online voting system using biometric characteristics, secure banking transaction are the application of visual secrete sharing scheme. Preprocessing of input image is performed if there

is a need of application. Then next step is to divide the input image into two or more share as per the need of application. Each share is then provided to the participants (this can be provided via email or any other application). Participants will now provide his share whenever needed. The provided share is then verified because sometimes fake or illegal share can also be provided by cheater or intruder. Finally verified shares are combined together and final image is formed. Problems such as pixel expansion, alignment problem, distortion, thin line problem occurred while combining the share are minimized using various error diffusion technique. Finally the quality of the image is improved and image is provided to required application for further processing.


Input an image that is to be secured
Perform Preprocessing if required
Divide the input image into two or more shares or parts as per the need of application
Key (A transparency)
Cipher Printed Page
Provide the share to each participants of the application.
Participants will now provide their share whenever required
Verify the provided share and check is it the genuine share or not, if the share is not genuine then stop the further processing and exit.
Combine the verified shares of the image
Minimizing the problems such as pixel expansion, distortions etc.

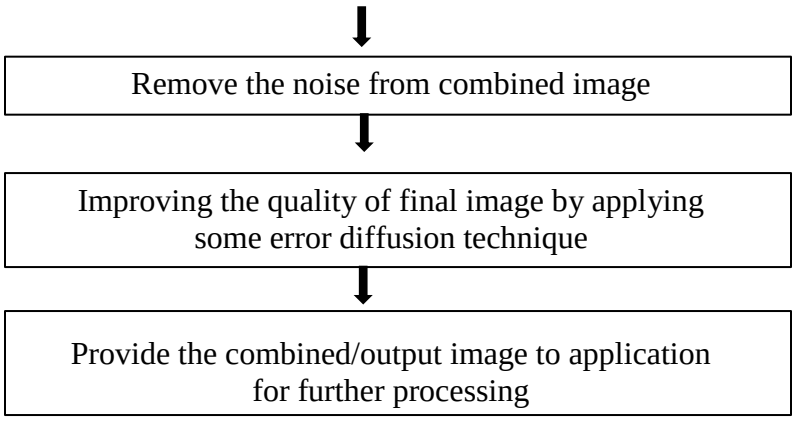

Remove the noise from combined image
Improving the quality of final image by applying some error diffusion technique
Provide the combined/output image to application for further processing

Figure 4.1: Proposed methodology

5. Importance of study/ Society application

i. International status.

Providing security to visual images is one of the most important issues discussed worldwide. Biometric security, online voting system, providing access to big data, more secure banking transaction, are some of the application of visual secrets sharing. So the Verifiable Color Visual Cryptography (VCVC) proposed for this study can be beneficial to all over the world for image security, sharing the secrets images over networks and allowing access to information based verifiable secrete share. The international status of the study will be impactful.

ii. National Status.

National status of the study will also be more impactful because most of the internet users in India rely on the networks security. Through this scheme they can use more users friendly, biometric based and more accurate mechanism for protecting the visual information. Also online voting system based on share allocated to voters can be more secure voting system and that is the need of voting system in India. Finally if the shares are verifiable then there will be 100% cheating prevision in final visual information.

iii. Significance of the study.

With the recent advancement in visual cryptography and secrete sharing scheme, it is possible to develop an autonomous system for image security and protecting information.

Providing verifiable shares for superimposing the shares and getting the final visual image is more important. So this study can be used to provide the most significant solution to the network users for protecting information in more secure way.

6. Proposed Work Design/Formulation and structure of study:

(Plan of work and targets to be achieved.)

Tentative phase wise plan of proposed study we have designed as per the convenience of the study.

Phase 1:

1. To provide the overview of the emerging Verifiable Color Visual Cryptography (VCVC) based on the previous related work.
2. To provide the efficient and more accurate solutions to various problems and different challenges of VCVC.

Phase 2:

1. To design and implement a new VCVC Scheme in order to secure an image transmission and cheating prevention for various types of images such as binary, gray, and color.
2. Minimizing the problems such as pixel expansion, distortions, flipping issues, cheating prevention and thing line problems of various secrete sharing scheme

Phase 3:

1. To Evaluate and analyze the performance of proposed VCVC Scheme to clarify is efficiency in comparison to recent related works.
2. Improving the quality of final image by applying some error diffusion technique.

Phase 4:

1. To enlist some of the application of newly developed scheme.
2. To contribute the commendation and assumption for the future development
3. Report Writing.

7. References

1. Moni Naor and Adi Shamir, "Visual Cryptography," Eurocrypt, 1994.
2. Young-Chang Hou “Visual cryptography for color images” Pattern Recognition Journal of the Pattern Recognition Society Volume 36, pp. 1619–1629,2002.
3. Jonathan weir and weiQi, Yan “Visual Cryptography and its Application”, Ventus Publishing Aps, eBook, pp.1-144, 2012.
4. Ecaterina Moraru , “Visual Cryptography”, Published in: Technology, Art & Photos on Slide share, pp. 1-38, 2008.
5. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo,” Halftone Visual Cryptography”, IEEE Transactions on image processing, vol. 15, no. 8, pp. 2241-2453, august 2006.
6. Zhongmin Wang, Student Member IEEE, Gonzalo R. Arce, Fellow IEEE, and Giovanni Di Crescenzo, “Halftone Visual Cryptography via Error Diffusion”, IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 383-396, September 2009.
7. Vandana Purushothaman and Sreela Sreedhar, “An improved secret sharing using XOR-based Visual Cryptography, Green Engineering and Technologies (IC-GET), 2016 Online International Conference, Nov 2016.
8. D. Jin, W. Q. Yan, and M. S. Kankanhalli, “Progressive color visual cryptography,” Journal of. Electron. Imaging, vol. 14, no. 3, pp. 1–13, 2005.
9. Young-Chang Hou and Zen-Yu Quan, “Progressive Visual Cryptography with Unexpanded Shares”, IEEE transactions on circuits and systems for video technology, vol. 21, no. 11, pp. 1760-1764, November 2011.
10. G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, “Visual cryptography for general access structures”, Proc.ICAL96, Springer, Berlin, 1996, pp. 416-428, 1996.
11. Abhishek Parakh and Subhash Kak “A Recursive Threshold Visual Cryptography Scheme”, CoRR abs/0902.2487, 2009.
12. Chang-Chou Lin, Wen-Hsiang Tsai, “Visual cryptography for graylevel images by dithering techniques”, Pattern Recognition Letters, v.24 n.1-3, 2003.
13. E. Verheuland H. V. Tilborg,”Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes.”Designs, Codes and Cryptography, 11(2), pp.179–196, 1997

14. F. Liu, C.K. Wu, X.J. Lin, “Colour Visual Cryptography Schemes”, IET Information Security, vol. 2,No. 4, pp 151-165, 2009.
15. C.C. Wu, L.H. Chen, “A Study On Visual Cryptography”, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.
16. S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, andK. Chen, “Sharing multiple secrets in visual cryptography”, Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.
17. Tzung-Her Chen n , Chang-Sian Wu,” Efficient multi-secret image sharing based on Boolean operations”, Signal Processing Volume 91, Issue 1, pp. 90-97, January 2011.
18. Nakajima, M. and Yamaguchi, Y., “Extended visual cryptography for natural images” Journal of WSCG. Volume 10, pp. 303-310, 2002.
19. Wang, R.Z. [Ran-Zan], “Region Incrementing Visual Cryptography”, SPLetters(16), No. 8, pp. 659-662, 2009.
20. Bernd Borchert, “Segment-based Visual Cryptography”, WSI ISSN 0946-3852,pp. 1-10, 2007.
21. Feng Liu · Wei Qi Yan,” Visual Cryptography for Image Processing and Security Theory, Methods, and Applications,” Springer, eBooks, pp. 1-154, 2014
22. Zheng D, Zhao Y, Wang J, “An efficient method of license plate location. Pattern Recognition Letter 26(15): pp.2431–2438, (2005)
23. Feng Liu, Teng guo, ChuanKun Wu , Lina Qian ,” Improving the visual quality of size invariant visual cryptography scheme”, Elsevier Journal of Visual communication Image R.23pp.331–342,2012.
24. Shivendra Shivani and Suneeta Agarwal, “VPVC: verifiable progressive visual cryptography”, Springer-Pattern Anal Application, https://doi.org/10.1007/s10044-016-0571-x, pp.1-28, July 2016.
25. Shivendra Shivani, “VMVC: Verifiable multi-tone visual cryptography”, Springer, Multimed Tools Application, https://doi.org/10.1007/s11042-017-4422-6, pp.1-20, January 2017.
26. Arun Ross, and Asem Othman, “Visual Cryptography for Biometric Privacy”, IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-82, March 2011

27. F. Liu C.-K. Wu," Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners", IET Inf. Security., Vol. 5, Issue. 2, pp. 121–128, 2011.
28. Yuh-Rau Wang, Wei-Hung Lin, and Ling Yang, "Lossless Watermarking Using Visual Cryptography Authentication", Proceedings of the 2013 International Conference on Machine Learning and Cyberetics, Tianjin, IEEE, pp. 1109-1113 July, 2013
29. Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Hiding Information in Document Images," Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489, 1995.
30. Souvik Roy and P. Venkateswaran," Online Payment System using Steganography and Visual Cryptography", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2014.
31. Wei-Qi Yan, Duo Jin, Mohan S Kankanhalli "Visual Cryptography For Print And Scan Applications", ,ISCAS, pp. 572-575, 2004
32. B.Srikanth, G.Padmaja, Dr. Syed Khasim, Dr. P.V.S.Lakshmi and A.Harith, "Secured Bank Authentication using Image Processing and Visual Cryptography", International Journal of Computer Science and Information Technologies, Vol. 5 (2), pp. 2432-2437, 2014.
33. Himanshu Gupta1, Nupur Sharma, "A Model for Biometric Security using Visual Cryptography", IEEE, pp.328-332, 2016
34. Angel Rose A , Sabu M Thampi," A Secure Verifiable Scheme for Secret Image Sharing 2015", Procedia Computer Science 58, pp.140-150, 2015
35. Mahmoud E. Hodeish, Linas Bukauska,Vikas T. Humbe," An Optimal (k,n)Visual Secret Sharing Scheme for Information Security", Elsevier- Procedia Computer Science 93, pp.760 – 767, 2016.
36. Ankush V. Dahata , Pallavi V. Chavan," Secret Sharing Based Visual Cryptography Scheme Using CMY Color Space",Elsevier, Procedia Computer Science, Volume 78, pp.563 – 570, (2016)
37. Rajendra A B and Sheshadri H S "Visual Cryptography in Internet Voting System", IEEE, pp. 60-64, 2013.

38. Kim, M., Park, J. and Zheng, Y. Human-machine identification using visual cryptography. In Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems, pp. 178-182. 1998
39. Wen-Pinn Fang," Offline QR Code Authorization Based on Visual Cryptography", IEEE Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 89-92, 2011.

Signature

Research Scholar
Mr. D. R. Somwanshi
School to Technology,
SRTM University Nanded,
Sub-Center Latur

Signature

Research Supervisor/Guide
Dr. Vikas T. Humbe
Assistant Professor
School to Technology
SRTM University Nanded,
Sub-Center Latur